Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-162 (Cancelled).

Claim 163. (New) A method for preventing unauthorized access to a specific resource within a computer network, comprising:

assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network;

assigning a unique user identifier (UID) to each authorized user of the network;

defining policy profiles for authorized computers and for authorized users of the network, wherein each policy profile identifies rights of access to resources within the network for the authorized users and the authorized computers;

upon initiation of a TCP/IP communication attempt for access to the specific resource, wherein the communication attempt is initiated by a specific authorized user logged into a specific authorized computer and wherein the communication attempt includes a synchronization packet having a SEQ and an ACK field, inserting the UID of the specific authorized user and the SID of the specific authorized computer into the SEQ and ACK fields of the synchronization packet;

intercepting the synchronization packet within the computer network;

extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt; and

allowing the communication attempt with the specific resource as a function of the policy profile of the specific authorized user and of the policy profile of the specific authorized computer.

Claim 164. (New) The method of claim 163 wherein the SID is assigned based on one or more constant identifiers obtained from hardware associated with the respective authorized computer.

Claim 165. (New) The method of claim 163 further comprising the step of encrypting the SID prior to inserting the SID into the synchronization packet.

Claim 166. (New) The method of claim 165 further comprising the step of decrypting the SID after intercepting the synchronization packet.

Claim 167. (New) The method of claim 165 wherein the SID is encrypted using at least one transformation key.

Claim 168. (New) The method of claim 167 wherein the transformation key is selected dynamically from a table of transformation keys.

Claim 169. (New) The method of claim 163 further comprising the step of encrypting the UID prior to inserting the UID into the synchronization packet.

Claim 170. (New) The method of claim 169 further comprising the step of decrypting the UID after intercepting the synchronization packet.

Claim 171. (New) The method of claim 169 wherein the UID is encrypted using at least one transformation key.

Claim 172. (New) The method of claim 171 wherein the transformation key is selected dynamically from a table of transformation keys.

Claim 173. (New) The method of claim 163 further comprising the step of recording the communication attempt in a database.

Claim 174. (New) The method of claim 163 further comprising the step of notifying a network administrator if the communication attempt is not allowed.

Claim 175. (New) The method of claim 163 further comprising the step of logging the communication attempt if the communication attempt is not allowed.

Claim 176. (New) The method of claim 163 wherein the specific resource is a database.

Claim 177. (New) The method of claim 163 wherein the specific resource is an application.

Claim 178. (New) The method of claim 163 wherein the specific resources is another authorized computer of the network.

Claim 179. (New) A method of monitoring a TCP/IP communication attempt within a computer network, comprising:

assigning a unique, non-dynamic system identifier (SID) to each authorized computer within the network;

assigning a unique user identifier (UID) to each authorized user of the network;

upon initiation of a TCP/IP communication attempt with a requested resource within the network by a specific authorized user logged into a specific authorized computer, inserting the UID of the specific authorized user and the SID of the specific authorized computer into SEQ and ACK fields of a synchronization packet associated with the TCP/IP communication attempt;

intercepting the synchronization packet within the computer network and prior to access of the requested resource;

extracting the UID and SID from the SEQ and ACK fields of the synchronization packet to identify the specific authorized user and the specific authorized computer initiating the communication attempt;

allowing the communication attempt with the requested resource to proceed; and

logging the communication attempt in a database to maintain a record of the specific authorized user and the specific authorized computer initiating the communication attempt.

Claim 180. (New) The method of claim 179 wherein the SID is assigned based on one or more constant identifiers obtained from hardware associated with the respective authorized computer.

Claim 181. (New) The method of claim 179 further comprising the step of encrypting the SID prior to inserting the SID into the synchronization packet.

Claim 182. (New) The method of claim 181 further comprising the step of decrypting the SID after intercepting the synchronization packet.

Claim 183. (New) The method of claim 181 wherein the SID is encrypted using at least one transformation key.

Claim 184. (New) The method of claim 183 wherein the transformation key is selected dynamically from a table of transformation keys.

Claim 185. (New) The method of claim 179 further comprising the step of encrypting the UID prior to inserting the UID into the synchronization packet.

Claim 186. (New) The method of claim 185 further comprising the step of decrypting the UID after intercepting the synchronization packet.

Claim 187. (New) The method of claim 185 wherein the UID is encrypted using at least one transformation key.

Claim 188. (New) The method of claim 187 wherein the transformation key is selected dynamically from a table of transformation keys.

Claim 189. (New) The method of claim 179 wherein the requested resource is a database.

Claim 190. (New) The method of claim 179 wherein the requested resource is an application.

Claim 191. (New) The method of claim 179 wherein the specific resources is another authorized computer of the network.